Indian J. Phys. 44, 71-90 (1970)

On wide-band communication techniques using pseudo-random and orthogonal sequences-I.

BY N. B. CHAKRABORTI, A. K. MUKHERJEE* AND N. PAL

Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology, Kharagpur, West Bengal

(*Received* 14 *October* 1966—*Revised* 11 *November* 1967, 30 *August* 1968 *and* 12 *January* 1970)

In this paper properties of pseudo-random and orthogonal codes are discussed. Methods of their generation and techniques of application of such codes for communication, simplifications of existing Modem by using techniques of maximum amplitude selection, time compression, code-frequency time-matrixing, sequential technique for estimation and decoding are briefly described.

1. INTRODUCTION

Considerable interest has recently been aroused in wide-band Communication techniques (Golomb 1965, Harmuth 1960, 1961, Chakraborti 1964, Costas 1959), which are finding application in space communications and telemetry, random access, and secure military communications. One well known reason for increasing emphasis on spread spectrum techniques is that when the signal to noise ratio is necessarily low the only way of ensuring reliable communication is to exchange time-bandwidth product for power. Such large WT communication techniques require that the time and band-width have been spread in such a way as to enable the signals received over a given transmission channel to be compressed in the receiver processor to occupy again the minimum time and frequency intervals of the modulation. The object of this paper is two-fold. (i) To briefly review some techniques of spread-spectrum communication and (ii) present some of our own work. In the second category how the spread-spectrum techniques can be combined with existing modulation methods and can also be used to develop new efficient methods of modulation are described.

An obvious way of increasing the frequency occupancy of a message waveform having a given bandwidth is to modulate a larger number of coherent carriers by the message. Evidently such coherent carriers could be replaced by any alternating waveform of known structure and bandwidth. Pseudo-random (P.r.) and orthogonal code sequences provide such waveforms. Properties of such sequences and methods of generating them are considered in Sec. 1.

* Present address: Institute of Radio Physics and Electronics, University of Calcutta, 92 Acharya Prafulla Chandra Road, Calcutta-9.

In time-frequency dispersal-accumulation techniques it seems imperative to employ pulse digital techniques for the purpose of matched filtering. Amongst pulse-digital modulation techniques M-ary, binary, pulse time modulation and delta modulation in conjunction with P.r. or orthogonal codes are discussed in Sec. II. Application of P.r. codes for determination of impulse response of a system is also discussed here.

Problems associated with synchronous as well as asynchronous multiplexing are considered in Sec. III. Techniques of synchronization in respect of the R.F. carrier phase, bit period and timing have also been discussed.

P.r codes find an important application in random access shared channel communication, where a large number of signals carrying different messages share the same channel, every user having immediate access to all other users without central switching and each user being capable of separating signals intended from the total traffic present. Problems of multiplexing in such addressing and modulation techniques are considered in Sec III. Waveform division multiplexing, time frequency matrixing, and code-frequency time matrixing applicable for binary PPM and DM are discussed.

It is felt that the quasi-Barker codes, the technique of maximum amplitude selection, code-frequency time matrixing and the sequential technique for decoding and estimation constitute useful new concepts.

2. P.R. SEQUENCES AND THEIR PROPERTIES

Processes characterised by unpredictable changes in time and exhibiting variations from observation to observation, which no amount of effort or control in the course of a trial can remove, are called random processes. However these processes also show regularities called statistical properties in a long series of trials. The statistical properties associated with random noise are the probability distribution of the amplitude and the auto-correlation function. In contrast, when a finite number of measurements of an ensemble determine the entire behaviour of the representative of an ensemble the process is called deterministic.

A pseudo-random time series is a deterministic time series having a finite number of states with known probability distribution, transition probabilities and specified transition times. The properties such a time series have in common with random noise are (a) an apparently bewildering complexity of wave form, (b) a peaked auto-correlatiion function and (c) a nearly zero average value if the time interval of observation is long compared with the correlation time.

It is known that the interval between the zero crossings of a noise waveform is a random function of time. It is not possible to regenerate such a characteristic and one has therefore to store the replica of transmitted noise waveform if any coherent reception technique is to be employed. Since each part of the noise waveform is unpredictable and the length of the sample of the noise waveform must be large compared to the correlation period, the storage capacity of the processor must be very large. Pseudo-random sequences, on the other hand, can be generated deterministically. Further the peak factor of those sequences can be made quite small. Hence for purposes of application, P.r. sequences are preferred to samples of noise waveform.

P.r. sequences are specified by the number of states (corresponding to binary, ternary, quarternary, etc. systems), the probability distribution of the states, the minimum time interval between two successive transitions and the length of the sequence. Pseudo-random sequences of binary digits with equal probability of the states have been investigated for reasons of simplicity and suitability for application. Here a sequence is designated as binary if it consists of two states, i e., presence and absence of a pulse (denoted respectively by 1 and 0).

Binary P r sequences can be generated by means of shift registers and modulo-two-adders. A device consisting of a consecutive binary storage positions, which shift the contents of each position, to the next in time, is termed a shift register A modulo-2 adder is a logic circuit, which gives with two inputs A and B the Boolean output $A\bar{B}+\bar{A}B$. If the two inputs differ *i e.*, (01, or 10) then we get an outut (1) and when the inputs are the same (11 or 00) then there is no output (0).

As an example one may consider a system consisting of a shift register with three storage positions and with the initial condition 101 and a mod-2 adder with its inputs from the first and third storage positions. If the output of the adder is fed back to first then for an initial condition 101 it goes through the succession of states 101, 010, 001, 100, 110, 111, 011, 101, ... and so on. The eighth state of course is the same as the initial condition set. So, at each of the shift registers and the modulo-2 adder we will get a sequence of ONES and ZEROS which repeat after a period of 7 units of the clock. At the three shift registers we will get outputs of (1001110), (0100111), ..., (1010011).

If on the other hand the inputs to the Mod-2 adder are the outputs of the second and third shift register, the sequence obtained is again of length 7, but assuming the same initial condition the output of the first shift register will be 0100011.

In general, the length of the sequence depends on the number of shift registers and the specific sequences obtained are determined by the logic.

It can be shown that the maximum period is $L = 2^n - 1$. The output sequences of this category are called maximal-length shift register sequences (Huffman 1956, Peterson 1961).

Special features of these sequences are :

(1) In each period numbers of zeros and ones differ by at most unity.

(2) Among runs of "one" and "zero" in the fine structure one-half runs of each kind are of length one. One fourth runs of each kind are of length 2, one-eighth of length 3 and so on.

(3) Mod-2 sum of two such sequences is another such sequence.

(4) If the period of such a sequence be considered term by term with any cyclic shift of itself, the number of agreements differs from the number of disagreements by at most one.

Generation of maximal length binary sequences

It has been discussed earlier how shift registers and modulo-2 adder can be used to generate the P.r. sequences. If the unit delay of the shift register be represented by D, then the law of formation of the sequence of length 7 is (a) $F(D) = I(+)D(+)D^3 = 0$ or $I(+)D^2(+)D^3 = 0$. The two conditions imposed give rise to two different sequences. The length of the sequence in both the cases is 7 (as $2^3-1 = 7$) and the the expression $I(+)D(+)D^3$ and $I(+)D^2(+)D^3$ are both prime factors. If the expression $F(D)$ can be factorized then that condition if imposed on a sequence generator will give rise to a sequence of length $2n^1-1$ where n^1 is the highest power amongst the factors.

Generation of any periodic sequence

As mentioned earlier, a shift register can be converted into a sequence generator by including a feedback loop, which computes a new term based on the previous terms. If the sequence is specified, it is in general possible to obtain from the truth table (table 1) the logic for generating a given sequence, starting from any permissible initial condition. The logic for maximal length sequence of length $L = 2^n-1$ is given below for several values of n.

TABLE 1.

No. of stages (n)	Length of sequence (L)	Feedback from stages
3	7	2,3 or 1,3
4	15	3,4 or 1,4
5	31	3,5 or 1,3,45 or 1,2,3,5
6	63	5,6
7	127	4,7 or 6,7
8	255	2,3,4,5
9	511	5,9
10	1023	7,10

Generation of sequence of periods given by $L < 2^n - 1$ is facilitated by the knowledge that all periods from 1 to 2^n can be obtained from an n stage register with approrpriate logic circuit. For example to obtain a sequence of length 11 one may start with a system for generation of a sequence of length 15 and derive appropriate output from a logical function generator to skip, route or recycle.

The block diagram for a sequence generator of length 11 or 13 is shown in figure 1.

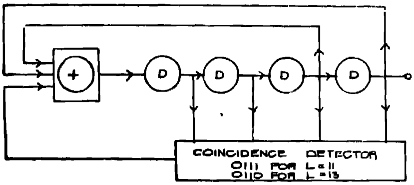

Figure 1. Schematic diagram of a P.r. sequence generator indicated mod-2-adder and D indicates delay unit. The coincidence detector is a logic circuit which gives an output (ONE) for the condition stated.

It may be mentioned that such sequence generators may be very conveniently used to count down by any factor.

To obtain sequences having large periods it is advisable to combine two or more sequences of smaller periods rather than realise it in a single stage.

When a sequence of a P.r. series passes through a band limited system (such as a filter) the shape of the pulses changes considerably. This change is maximum in case of transitions and is obviously small when the same state (one or zero) is continued. Such waveform distortion results in a considerable departure of the correlator output from the desired. This difficulty can be overcome if we can so arrange that the unit signals in every bit period are identical. In this case the change of shape is uniform for each bit and so all the properties of combinations of the series remain unaltered. This can be accomplished if we sample the series by pulse train of equal repetition rate but of shorter duration.

Optimum correlation code for time modulation or ranging (Barker and Quasi-Barker codes)

Some members of P.r. codes have the property that the correlation side lobe in the matched filter output is quite small. Barker(1953) has shown that there are sequences for which the correlation side lobe is as small as $1/L$. Such sequences are known only for length $L = 3, 7, 11$ and 13. It is possible to combine two or more Barker sequences to generate a new sequence in the following way. A sequence of given length (m) forms group or block. A new sequence of length (n) is then constructed taking this group as a unit. Unfortunately, the side lobe amplitude in such case is rather high, being the larger of $1/m$ and $1/n$. It seems therefore useful to enquire whether long sequences exist for which the minimum correlation side lobe is restricted to $2/L$ or $3/L$. The study shows that some P.r. sequences have such property *e.g.*, for sequence of length 19, (1001001100001010111) matched filter output is 1, 0, -1, -2, 1, -2, -1, 2, -1, 0, -3, 0, 1, -2, 1, 0, -1, -2, 19. Similarly, for sequence of length 23 (0110, 0110, 01010000, 1111101) matched filter output is -1, 2, -1, -2, 1, 2, -1, 0, 1, 0, -3, 2, -1, -2, -1, 0, -3, -2, 1, 0, -3, 0, 23). Such sequences are grouped here as quasi-Barker sequences.

Orthogonal codes and their properties

It has been observed earlier that the cross-correlation output between any two signals of the same family of P r. sequences is $1/L$. There is another class of signals which have zero cross-correlation between them. These are called orthogonal signals.

The most familiar example of an orthogonal code is a trigonometric orthogonal code. But in case of these type of codes the peak factor is large. Binary orthogonal codes are available which have very good peak factor. Such codes are generally related to orthogonal matrices which have been discussed by Paley and others. Paley (1933) has shown that orthogonal matrices of order m can be formed if either of the following conditions is satisfied.

(a) $m = 2^k$

(b) $m = p+1$, p is a prime and $p = 3 \pmod 4$

(c) $m = 2^k(p+1)$, p is prime.

(d) $m = 2^k(p^h+1)$, p is an odd prime, m is divisible by 4.

Instead of quadratic residue (mod p) we consider quadratic residue in Galois field of polynomial, (mod p_0, mod $f(x)$) where $f(x)$ is an irreducible polynomial of degree h. Thus for instance . $p^h = 3$ mod(4) $k = 0$.

(e) $m = 2^k p(p+1)$, $p = 3 \pmod 4$ and p is prime.

Let us consider an example of an orthogonal matrix belonging to group (b), i.e., $m = p+1$, where p is a prime number and $p = 3 \pmod 4$. The coefficient Aij of the orthogonal matrix will be taken to be 1, if $(i-j)$ satisfies the condition that it is a quadratic residue of the prime number, *i.e.*, if a number x(say) such that $x^2-k = 0 \pmod p$ exists, where k equals $(i-j)$. Further Aij may be taken to be equal to -1 and A_{i0} or A_{0i} is equal to 1. One row of the orthogonal matrix constructed in the manner indicated with $m = 12$ can be represented as 111100010010.

If we require the signals to be resolved in fequency then we will choose such signals which have power spectrum distinct and different for different members of the codes. But if we require resolution in time then the power spectrum should be the same for different codes but they should have distinct wave-shapes with reasonable separability in time.

P.r. sequence can never be used where we require resolution in frequency but orthogonal code can be used for both. It will be observed that while orghogonality is independent of interchange of columns, the actual value of the cross-correlator output for a given shifts may be minimised by such interchange.

Generation of orthogonal codes

As mentioned earlier orthogonal trigonometric codes may be generated by combining trigonometric functions which have the same fundamental periods. Obvioulsy the functions $\cos wt$, $\cos 2wt$, ... $\cos nwt$, $\sin wt$, $\sin 2wt$ ... $\sin nwt$ are mutually orthogonal. Linear combinations of these functions will also be found to be orthogonal if appropriate weighting factors are used. For instance

$$f1(t) = \cos wt + \cos 2wt + \cos 3wt + \cos 4wt \quad \text{and}$$

$$f2(t) = \cos wt - \cos 2wt + \cos 3wt - \cos 4wt$$

are mutually orthogonal.

The difference between primary and combination functions is that the spectral regions occupied by the primary functions are different while for the combination functions the spectral regions occupied overlap.

Binary orthogonal sequences can be obtained by combining short pulses of appropriate duration, sign and delays to obtain different codes. One obvious method of obtaining several short pulses is to excite a number of monostable multivibrators in a chain, each pulse being generated from the trailing edge of the previous pulse and then to add them with proper sign.

An easier approach to this problem, as shown in figure 2, is to use the waveform obtained from dividers formed by a chain of bistable multivibrator operated serially, these waveforms constituting members of an orthogonal family. The rest of the members are obtainable from mod-2 sum of the primary members. This type of system can produce code family of length $L = 2^n$.

If the length $L \neq 2^n$, then this idea is no longer suited. However, a general technique is available for generating binary orthogonal codes. This consists of adding a single pulse of proper polarity at the start of a P.r. code of length $(L-1)$. The first position of these codes is always the pulse added, whereas the next $(L-1)$ positions correspond to the one of the P.r. sequences. This idea can also be extended for sequences having length $L = 2^n$.

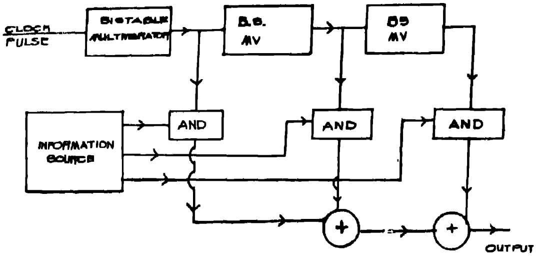

Figure 2. Schematic diagram of an orthogonal sequence generator employing binary flip-flops and logic circuits.

3. Communication by P.r. codes

We have already observed that P.r. and orthogonal sequences have the following important properties—(a) these permit time-compression by a very large factor and have good resolution in time, it being possible to resolve sequences separated in time by an interval equal to the period, (b) sequences belonging to the same family and synchronous in time can be separated out with little or no mutual interference, and (c) it is possible to accumulate the signal voltages of all the individual signals spread over in time, so that the signal strength at the instant of matching is equal to LS where L is the sequence length and S is the signal voltage in any bit period, while the resultant noise voltage due to incoherent summation will be equal to $\sqrt{L}.N$ where N is the noise voltage in any bit period. These properties recommend the use of such sequences particularly in situations where signal to noise ratio is very small for ranging application and time modulation, waveform multiplexing in binary modulation and the so-called M-ary modulation.

In this section we wish to discuss the application of wideband codes P.r. or orthogonal, for communications and the advantages arising from such applications.

M-ary Modulation

We shall first consider M-ary modulation technique which is known to be an optimum coding method. In M-ary modulation, one of M alternative sequences is transmitted at a given time in accordance with the given state of the message source. These sequences, like samples of noise waveform, have little or no cross correlation if the integration is carried out over the appropriate time interval. In the receiver the decision with regard to which sequence has been sent is made on the basis of the comparison between the outputs of M correlators. For speech signal, analogue speech signal is first sampled and quantized and then the sampled signal is converted into pulse code. This p.c.m. code is now used as the initial condition of the P.r. sequence generator or orthogonal sequence generator. Thus we get different sequences according to different amplitudes of the sample speech signal.

The technique of reception and decoding almost always employs matched filtering technique. In this type of reception we shall require as many receiver processors as there are possible sequences, a particular processor corresponding to a specific sequence. The decision with regard to which sequence has been transmitted will have to be made on the basis of magnitude of the output of the matched filters and the sequence that gives the largest output will be selected. A correspondence between the line selected and the analogue voltage may then be established.

To decide which sequence has been transmitted, the technique available is to use the parallel detection method where the received input signal is multiplied with all the possible sequences and the averges of the multiplied outputs are noted. The average of the multiplied outputs are sampled and the samples are fed to a decision circuit to determine which has the maximum value. This maximum is an indication of which sequence has been transmitted. Figure 3 shows the mechanization of a maximum likelihood decoder. For such a decoder we will require as many multipliers, integrators and samples as there are possible sequences. The size of the decoder becomes unwieldy if the number of sequences is large.

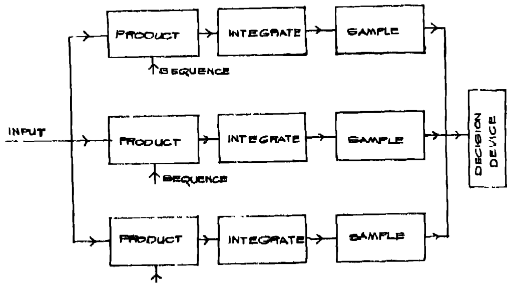

Figure 3. An optimal parallel decoder for M-ary modulations.

The size of the decoder can be minimised to a great extent if we use the serial technique in which the signal is compressed in time by means of a time compressor (Weber 1964), the compressed signal is stored and correlated with the different time shifted versions of the receiver P.r. sequence serially, the correlation outputs occuring serially being then examined for maximum amplitude. To achieve this the time of occupancy of each original signal component must be reduced to at least T/n, where n is the number of samples to be accommodated.

In such a technique of detection, the number of multipliers, integrators and samplers can be reduced to one only, whatever be the possible number of sequences to be received. In the parallel detection method one must have all the time shifted replicas of the sequence present simultaneously. Such a scheme is purely impractical especially when the length of the sequence is large. But in the case of serial decoding as one will be testing the sequence serially, the receiver sequence generator need be the conventional maximal length sequence generator. The schematic diagram for such a detection technique is shown in figure 4.

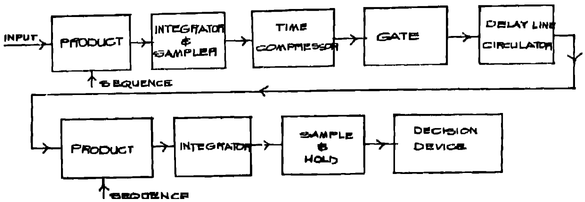

Figure 4. Schematic diagram of a serial decoder for M-ary modulation.

The received signal is first integrated and the integrated outputs at the end of each bit are sampled and these samples are then compressed in time. If T secs be the bit period of original sequence of length L then after the time compression each sequence will only be occupying T secs. Then this compressed sequence whose period is also T has bit period T/L. It is clear that for such processing we are to have the input received sequence present for a period till all the time shifted replicas of the sequence are tested. For this purpose we use a delay line type circulator whose delay is equal to $T(1+1/L)$. This enables correlation of the input in the receiver sequences time shifted by units of one bit period. After all the sequences are serially tested we require the circulator to be discharged and ready for testing of the next sequence. Now the minimum discharge time of a delay line is equal to the amount of delay produced by it. So, the total time taken for a full operation is $(LT+2T)$, $(LT+T)$ for testing and approximately another T for discharging Thus while the coding is done we must have a gap of $2T$ seconds after each sequence of period nT seconds.

The output of the multiplier is integrated and sampled at instants of matching for the different sequences and stored. When all the results have accumulated the same decision technique as used in the case of parallel method is employed.

Maximum amplitude selection

In M-ary communication the decision process involves determination of the particular code word on the basis of comparison between the output of matched filters. This requires selection of line giving maximum amplitude from amongst

M lines. The similarity to selection diversity switching may be noted here. For the purpose, all the line amplifiers should have an automatic gain control arrangement operated by the average amplitude. This type of common degeneration may be combined with individual amplitude dependent regeneration for accentuating the difference in level between the outputs of different lines. If it so happens that even after such treatment more than one line has an output exceeding the threshold, the amplifiers associated with this may be biased by the average of the outputs to eliminate all but the strongest component.

One technique which seems promising is to use multi-level *FM* in the receiver, that is, to use the outputs of the different 'alphabet' channels to amplitude modulate a set of carriers displaced in frequency and utilize strong signal capture phenomenon for the threshold decision circuit

Binary modulation

In case of binary modulation there will be only two states to transmit. These two states may be (a) a sequence or its absence, (b) alternate polarity of the same sequence, and (c) one of two orthogonal sequences.

Amongst these bipolar mode seems to be the desirable mode of operation. The two-sequence mode results in a more complex receiver, while off-on mode does not give the best SNR In the bipolar mode the selected sequence will have a positive polarity for a positive polarity of the input, the sequence generator being timed in accordance with the timing sequence of the transmitter. In such operation it is desirable to select a Barker (1953) type code for the sequence, for such codes have the best available correlation properties. In the receiver one need have a matched filter matched to the particular Barker code transmitted and the reception technique must be a synchronous one suited for reception of bipolar signals.

Pulse position modulation

As mentioned earlier P.r codes having very good resolution in time are eminently suited for use in ranging and hence in pulse position modulation. For obtaining P P.M signals analogue speech signal is first processed by a threshold circuit to remove voltage below a certain amplitude. This processed signal is now amplified and sampled. The sampled signal is then used to position modulate the pulses. If now the position modulated pulses are used to trigger the P.r. sequence generator (preferably a Barker code) then we will get sequences having the starting point varying in proportion to the amplitude of the sample.

In case of reception the knowledge of which sequence is being transmitted must be built into the receiver. The receiver is to decide from the correlator output about the starting time of the sequence. Here one may usefully employ matched filter technique to find the time of occurrence of the maximum amplitude of pulse.

A method of determining this is to use the technique of a voltage saw-tooth reset by the matched filter output. In this case a saw-tooth wave generator is triggered at the beginning of each frame The matched filter output pulse if it exceeds certain threshold level is used to reset the saw-tooth wave generator. The maximum amplitude obtained by the saw-tooth generator is then a measure of time of occurrence. Such a simple technique is directly applicable provided the probability of spurious signal exceeding the selected threshold is very small. A modification of the above for finding the time of occurrence of a pulse having the maximum amplitude in a selected time interval in the presence of spurious pulse and interference is however available. In this case the input pulses are applied to a peak charging diode; if the incoming pulse has an amplitude greater than the value of the voltage across the peak measuring device, a pulse of short duration is generated by the comparator. The output of the comparator is used to reset the free-running saw-tooth generator. The synchronised voltage for the saw tooth generator is obtained from p r.f. generator as in figure 5.

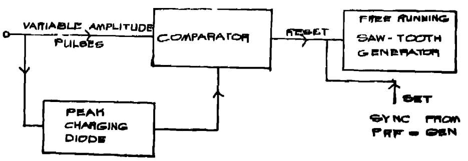

Figure 5. Arrangement for selecting the pulse having maximum amplitude.

Delta modulation

P.r. or orthogonal codes may be employed with any pulse modulation system by replacing the single pulse ordinarily used by the sequence. The additional unit required in such a case is a matched filter at the receiver. In the case of Delta modulaton ($\Delta-M$) or Delta-Sigma ($\Delta-\Sigma$) the pulse obtained from the conventional modulator may be used to obtain P.r. or orthogonal sequences of desired length. It should be observed that time gating for synchronous $\Delta-M$ in the output of the matched filter of the receiver provides in this case a very useful technique of interference reduction. In fact $\Delta-$M is indeed a viable technique for random access. It is the simplest analogue to digital conversion technique and has all the well known advantages of digital communication. It has a low pulse rate and low duty cycle compared with other digital modulation. Further, one has only to transmit pulses of one polarity and techniques for removal of redundancy can be readily incorporated which together enable realization of a duty factor of about 0 30.

P.r. sequence as a test signal

It is well known that impulse response of a linear system can be determined by cross-correlating the input and the output if the input is white noise. From the convolution theorem one has

$$y(t) = \int_0^\infty x(t-t_1)h(t_1)dt_1$$

where $y(t)$ and $x(t)$ are the output and the input respectively and $h(t)$ is the impulse. Multiplying both sides by $x(t-\tau)$ and integrating one gets,

$$\phi_{yx}(\tau) = \int \phi_{xx}(\tau-t_1)h(t_1)dt_1$$

if $$\phi_{xx}(\tau-t_1) = \delta(\tau-t_1), \quad \text{then} \quad h(\tau) \approx \phi_{yx}(\tau).$$

It is obvious that pseudo-random waveforms with their highly peaked autocorrelation function approaching a delta function provide a better alternative than pure noise signals for the purpose of system idetification, because of the simplicity of generation, storage and processing of the experimental data.

3. Multiplexing and random access

Pulse-digital modulation systems may be classified as synchronous or a synchronous according as there is time synchronism between the events or not, *i e.* the time of arrival of the signal or the instant of time when the transition occurs in a precisely known period.

Channels are ordinarily multiplexed by means of either frequency division or time division multiplexing. A different technique of multiplexing can however be realized by means of orthogonal or pseudo-orthogonal codes in combination with time frequency matrixing. This type of multiplexing is usually asynchronous as its operation does not depend on allocation of specific time slots to the different signals and their synchronous routing at the receiving terminal.

Asynchronous systems find use in so called "Random Access" communication. In a random access system signals arise from sources dispersed in a random manner in location and time and users are allowed access as desired to a wide band channel and should be able to separate signals intended for them from the common channel. Obviously, the multiplexing here must also include a type of "addressing".

We intend to discuss here the technique of multiplexing that may be employed for binary modulation, P.P.M. and $\Delta - M$.

In case of binary modulation one may use what may be called waveform division multiplexing where different signals in the channel are allocated specific waveform codes. These waveform codes are selected in such a way that the filters matched to the different waveforms at receiving end are able to select only the desired wave and reject the others. An important parameter in this connection is the peak height of the mutual correlation between the different wave-forms, which obviously must be kept below a certain maximum. This consideration precludes the use of members of pseudo-random code derived, for example, from a maximal length sequence unless only a few of the total number of possible sequences which are widely separated in time are used.

Further it is found that even for orthogonal codes the maximum value of the cross-correlation output may be as large as $L/2$, where L is the length of the sequence, although the output of the correlator due to any undesired code is zero at the instant of matching. This causes severe mutual interference in asynchronous code division multiplexing. This problem is absent in synchronous multiplexing as in this case the outputs are observed only at precisely known instant of matching. One may in a large measure remove this difficulty by using time frequency matrixing, where code modulated bursts at different frequencies are arranged in a specific order in time for a given signal. Consider that the total signal time is divided into three intervals T_1, T_2, and T_3 which can be occupied by pulsed sinusoids of frequency f_1, f_2, and f_3. For a particular channel one may allocate the matrix element f_1T_1, f_2T_2, and f_3T_3. At the receiver particular signal can be selected by delaying the output at frequency f_1, f_2 by T_3-T_1 and T_3-T_2 and combining the output at three frequencies. The resultant output will obviously be large, only for this particular matrix element. For combining the outputs two approaches are available-predetection and post detection combination. In the case of predetection combination, the r.f. outputs at the three frequencies may be brought to the same frequency and phase lock circuits may be employed to phase the three signals and add them. The combined output is then fed to the matched filter detection and decision circuit. In the case of post detection combination the outputs at the three frequencies are fed to the matched filter detected, added and applied to decision circuit.

The above mentioned multiplexing technique can be employed in channels using binary phase-shift keying (PSK). In the case of code division multiplexing, it is necessary to distribute the static phases of the carrier uniformly over 2π radians in order that the peak factor of the sum signal could be kept within a reasonable limit. It is instructive in this connection to find the mean, r.m.s. and peak of the amplitude of the sum of N bipolar voltages (a) if the r.f. reference phase is the same for all and (b) if the r.f. phases are distributed uniformly for 2π radians.

For P.P.M. system using P.r. codes several techniques of multiplexing are available. One may for example use different codes obtainable from a code generator for multiplexing the channel. The code selected should obviously be such as to give rise to small mutual interference. The advantage arising from such multiplexing is that the amount of permissible range of time modulation is large and is given by T_r-LT where T_r is the repetition period, L the length of the

TABLE 2

	N = 4		N = 6		N = 8	
	(a)	(b)	(a)	(b)	(a)	(b)
Max	4	2.8	6	$\sqrt{12}$	8	5.2
rms	2	2	$\sqrt{6}$	$\sqrt{4.5}$	2.19	2.8
mean	3/2	7/4	15/8	15/8	3.43	2.4

sequence and T is the bit period. Further, such a system does not require synchronization and can therefore be used for random access communication. There will however be some amount of mutual interference between the channels, the magnitude of which will depend on the total number of active channels at a given time, the cross-correlation property of the codes and the signal statistics at different channels. It should be reasonable to expect that the different signals arising from different sources will be uncorrelated and consequently the actual interference can be thought of as due to randomly time modulated pulse trains. Time frequency matrixing using the same code, preferably a Barker or a quasi-Barker one may also be employed.

It should be realized that sometimes different interfering signals together may give rise to particular f t ordering of code thus producing a false output. To reduce the amount of false output one has to select only a limited number of possible combination of $f-t$ codes which can be formed with the given set of frequencies.

Code-frequency-time matrixing

In frequency time matrixing, the distinct addresses available depend on the number m of distinct frequencies used. Although this number would appear to be large, the actual usable combinations are rather few if false addressing is to be kept low. For example, using three frequencies one finds that acceptable combinations are instead of eight only three, provided by the cyclic permutation *i.e.* (f_1t_1, f_2t_2, f_3t_3), (f_2t_1, f_3t_2, f_1t_3) and (f_3t_1, f_1t_2, f_2t_3). It will be observed that the contribution from any interfering source to the desired address is at least $1/m$ times the correlation peak, where m is the number of frequencies used. Identical remarks apply, *mutatis mutandis*, to code time matrixing.

In code-frequency-time matrixing one can take advantage of the quasi-orthogonality between the selected code and frequency-time ordering to realize combination addresses with very small mutual interference. If we take three mutually orthogonal codes and three distinct frequencies the following three combinations $(M_1f_1t_1, M_2f_2t_2, M_3f_3t_3)$, $(M_3f_2t_1, M_1f_3t_2, M_2f_1t_3)$ and $(M_2f_3t_1, M_3f_1t_2$

$M_1 f_2 t_3$), obtained by taking the diagonal elements of the admissible M and f matrices, will be found to have excellent resistance to interference.

Synchronization

A digital receiver requires timing information in order to interpret the received signal sequences properly; when the value has become fully, each symbol in the sequence must be sampled at a time established and is not in a condition of transition

It will be recalled that an optimum receiver correlates received code word with the locally generated replica. Consequently, the instant in time in which one received word ends and the successive word begins must be known accurately. Besides, a suitable carrier for coherent demodulation must also be established and maintained. Thus there are three parameters to be synchronized, r.f. carrier, phase and frequency, word timing and bit timing. Techniques of r.f. synchronization are quite well established (Chakraborti & Biswas 1964, Chakraborti & Dutta 1966, 1967, Chakraborti 1964, Costas 1959) and will not be considered here.

To find word timing an automatic time control arrangement using a differential coincidence circuit may be used. In such a case one finds two correlations : (a) the correlation $R_1(t) = \overline{f_t(t)f_r(t)}$ between the input $f_t(t)$ and the replica at the receiver $f_r(t)$ and $(b) R_2(t) = f_t(t)[f_r(t-T)-f_r(t+T)]$ where T is one bit period. The product of these correlations is then used to control the timing of the function. Such a technique may be termed self-synchronizing technique. Another technique is to insert an auxiliary synchronizing pattern periodically in the channel. If a pattern is chosen which cannot occur as part of the data sequence then position identification of the pattern establishes synchronization. It is obviously desirable to make the correlation between all the data sequences and the synchronizing pattern as small as possible. A satisfactory synchronizing pattern is one which gives very small output of the matched filter except at the instant of matching. Use of Barker sequence and quasi-Barker sequence seem appropriate here.

For synchronization when bipolar modulation with a single Barker or quasi-Barker code is employed the arrangament shown in figure 6(a) may be used. When the signal as transmitted contains the code component, that is, the transmitted signal is obtained by mod-2 addition of the code and the clock, the arrangement marked may be used. Another r.f phase lock circuit applicable for bipolar phase modulation is shown in figure 6(b).

Sequential technique

An important consideration here is the time required to effect acquisition of the code or synchronization. The Auto-correlation function of a P.r. sequence does not provide any indication during the search process of which way or how

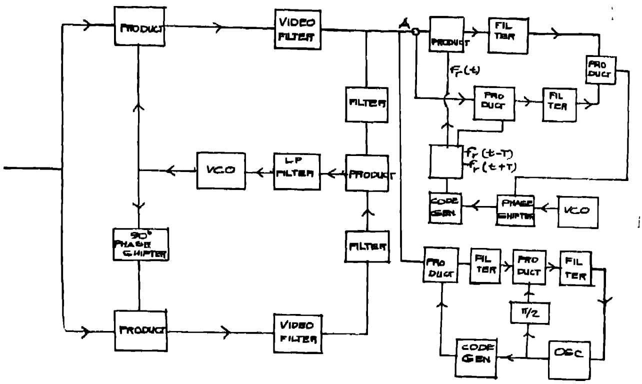

Figure 6(a) Schematic diagram of a circuit for achieving R.F. Phase look and synchronization of the bit period and timing. Circuit to the left of A represents a typical phase lock circuit for bipolar A M.

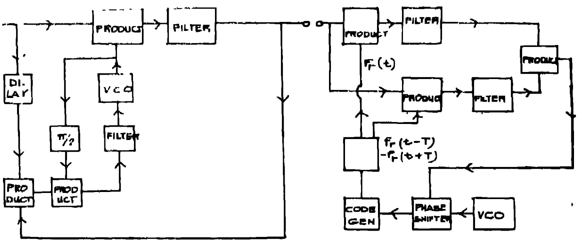

Figure 6(b) An alternative form of the phase lock circuit for bipolar modulation.

far to shift the local replica in order to bring about coincidence once it is outside the working zone. One has therefore to make trial correlation and find which code-shifts yield the highest correlation. The acquisition time therefore is rather very high compared to the information bits ($\log 2L$), while in the absence of noise the sequences is completely determinable from one trial inspection of n digits. When the signal energy relative to the background noise is sufficiently high, the number of trials can be sufficiently reduced if the code is made up of several short sub-codes that can be acquired individually.

It will be recognized that in the absence of noise optimum acquisition technique is to introduce the first n received bits as the initial conditions of the receiver sequence generator which will then continue to produce a sequence approximately in phase with the incoming sequence. Errors arising may be corrected by the tracking loop. However as the input invariably contains noise, it is necessary to find, by means of cross-correlation between the input sequence and the receiver sequence, whether initial estimate is correct. If the agreement between the two is not good, new data may be introduced and the process repeated in such a way as to (taking advantage of the longer integration time) enable rapid acquisition. New trials made on introduction of the new data need not destroy the information obtained from earlier trials. In such sequential estimation technique the length of the trial, which must be kept above a minimum to avoid false alarm and false dismissal, depends upon input signal to noise ratio. The acquistion time can therefore be kept small if the SNR is adequate.

Matched filter technique

Matching means optimization of a receiving system to extract the desired signal from a noise background maximising the signal to noise ratio. In essence matched filter technique is the same as correlation detection technique. There is a variety of ways by which the optimization process can be physically effected but some of them can be thought as correlators and others as matched filters.

The matched filter processors depend on (1) the nature of the signal, (2) the accompanying noise statistics and the way it combines with the signal and (3) the optimization required. The first two are essentially *a priori* data and the third one is the choice of criterion. Generally, the choices are all based on the energy calculation, *i.e.*, on some form of maximization of signal energy to that of the noise. Usually the matched filter design is obtained by maximization of signal to noise ratio (S/N matched filter).

Matched filter for a specific binary sequence

When the specific binary sequence of length L is being received the output of the matched filter at the instant of matching must equal L times the amplitude of each unit. This requires that the impulse response of the matched filter be a time reversed replica of the input sequence. For a binary sequence of 0100111 (zero signifies negative polarity) the impulse response of the matched filter must be 1110010. The output of the matched filter is then -1, 0, -1, 0, -1, 0, 7, 0, -1 0, -1, 0, -1.

Such matched filter may be easily realized by means of delay line having seven taps, with the delay between consequetive taps being equal to the delay between unit signals of the binary sequence, and the output obtained at the different taps being combined with appropriate polarity.

It is well known that a tapped delay line with resistor weights at each tap constitutes a linear filter. The array of resistors with different amplifiers for obtaining positive and negative value represents the impulse response of the filters.

The delay line accepts the incoming signal translating it across the spatially distributed resistor weights. The maximum output at the adder occurs at the instant when the desired signal fills the delay line.

The delay line may take a variety of forms (i) analogue LC or ultrasonic delay line or (ii) digital delay line. The ultrasonic delay line is essentially a band pass delay line and may consist of an array of barium titanate transducers coupled to any sonic solid media having small dispersion. If the input signal is translated down in frequency to video infinitely clipped and sampled then the analogue delay line may be replaced by a digital delay line such as shift register, operated by a clock having a repetition period equal to the required unit delay. The advantage of a digital delay line is that at each tap (trigger stage) the signal is regenerated and that precise timing can be achieved consistent with accuracy inherent in digital technique. Digital shift register permits the realization of extremely long high speed matched filter. Further the system is very readily adjustable for variable bit period while this poses a serious problem in any analogue delay line. The principal disadvantage is that as the input signal at a relatively low level has to be clipped, threshold effect causing suppression of the signal by the noise sets in. Finally for a band pass matched filter two video matched filters one each for the two quadrature channels will be needed.

Concluding remarks :

In this paper we have discussed only the basic concepts involved in the utilization of P.r and orthogonal codes in spread spectrum communication. Detailed experimental investigation of the concepts and practical embodiment of such utilization will be described in communications to follow. One point may still be made. The problem of generation and encoding is quite simple; the decoding technique on the other hand is quite complex. It would seem desirable to concentrate efforts on serial decoding (section 2) and sequential estimation aimed at simplification of circuitry and reduction of processing time.

Acknowledgement

A part of this work was done at the Institute of Radio Physics and Electronics, Calcutta. The authors are grateful to Prof. G. S. Sanyal for his kind interest and encouragement. Their thanks are due to Dr. J. Das and Mr. R. C Ganguli for helpful discussions.

References

Barker, R. H. 1953 *Communication Theory*, W. Jackson (Editor) Butterworths Scientific Publications, London, 273.

Chakraborti, N.-B. & Biswas, B.N. 1964 *Indian J. Phys.* **38**, 148.

Chakraborti, N.B. & Dutta, A.K. 1966 *Indian J. Phys.* **41**, 501.

Chakraborti, N.B. & Dutta, A.K. 1967 *Indian J. Phys.* 41, 87.

Chakraborti, N.B. 1964 *Proc. I.E.E.E.* **52**, 1248.

Costas, J. P. 1959 *Proc. I.R.E.* **47**, 2058.

Golomb, S. W. 1965 *Digital Communication with Space Application.* Prentice Hall Inc. Englewood Cliffs, N. J.

Harmuth, H. F. 1960 *Proc. I.E.E.*, **107**, 242, Monograph No. 369E.

Harmuth, H F. 1961 *Proc. I E.E.*, **108**, 139, Monograph No. 405E

Huffman, D. A. 1956 *3rd. London Symposium on Information Theory.* Cherry Ed. Butterworths Scientific Publications, London, 77

Middleton, D. 1960 *Statistical Communication Theory.* Mc-Graw Hill Book Co. New York.

Paley, P. E A C 1933 *Journal of Mathematics and Physics.* **12**, 311.

Peterson, W. W. 1961 *Error Correcting Codes.* John Wiley Sons Inc.

Shannon, C. E. 1949 *Proc. I R.E.* **37**, 10

Weber, S. 1964 *Modern Digital Circuit.* Mc-Graw Hill Book Co., New York.

Woodward, P. M. 1955 *Probability and Information Theory with Application to Radar.* Pergamon Press Ltd , London.